KELLEY DRYE & WARREN LLP

A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400 3050 K STREET, NW WASHINGTON, D.C. 20007-5108

PARSIPPANY, NJ

(202) 342-8400

DIRECT LINE: (202) 342-8614

FACSIMILE

(202) 342-8451

www.kelleydrye.com

EMAIL: dsmith@kelleydrye.com

BRUSSELS, BELGIUM

NEW YORK, NY

CHICAGO, IL

STAMFORD, CT

AFFILIATE OFFICES
MUMBAL INDIA

March 1, 2010

VIA ECFS

Marlene H. Dortch Office of the Secretary Federal Communications Commission 445 12th Street, S.W. Washington, DC 20554

Re:

Annual Customer Proprietary Network Information Compliance

Certification; EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to 47 C.F.R. § 64.2009(e), One World Telecom, LLC ("One World") and Yo Llamo, LLC ("Yo Llamo) (jointly, the "Companies") hereby provides its 2010 Annual Customer Proprietary Network Information Compliance Certification. Please feel free to contact me if you have any questions regarding this filing.

Respectfully Submitted,

Denise N. Smith

Counsel to One World Telecom, LLC and Yo Llamo, LLC

cc: Best Copy and Printing, Inc. (via e-mail)

Annual Customer Proprietary Network Information Certification Pursuant to 47 C.F.R. § 64.2009(e) EB Docket No. 06-36 February 2010

Annual 64.2009(e) CPNI Certification for 2010 covering the prior calendar year 2009

Name of Company(ies): One World Telecom, LLC and Yo Llamo, LLC

Form 499 Filer ID:

824860, 827252

Name of Signatory:

Jorge Asecio

Title of Signatory:

President

I, Jorge Asecio, certify that I am an officer of One World Telecom, LLC ("One World") and Yo Llamo, LLC ("Yo Llamo) (jointly, the "Companies") and acting as an agent of the Companies, that I have personal knowledge that the Companies have established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 et seg.

Attached to this certification is an accompanying statement explaining how the Companies' procedures ensure the Companies are in compliance with the requirements set forth in sections 64.2001 et seq. of the Commission's rules.

The Companies have not taken any actions (instituted proceedings or filed petitions at either state commissions, courts, or at the FCC) against data brokers in the past year. The Companies have no information outside of Commission Docket No. 96-115, or that is not otherwise publicly available (e.g., through news media), regarding the processes pretexters are using to attempt to access CPNI. The steps the Companies have taken to protect CPNI include updating their CPNI practices and procedures and conducting new training designed to ensure compliance with the FCC's modified CPNI rules.

The Companies have not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Jorge Asocio

President-

One World Telecom, LLC and Yo Llamo, LLC

Date:

Customer Propriétary Network Information Certification Attachment A

The Companies have established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("FCC") rules pertaining to customer proprietary network information ("CPNI") set forth in sections 64.2001 – 64.2011 of the Commission's rules. This attachment summarizes those practices and procedures, which have been updated so that they are adequate to ensure compliance with the Commission's CPNI rules, as modified by the Commission in 2007.

Safeguarding against pretexting

The Companies take reasonable measures to discover and protect against attempts to gain
unauthorized access to CPNI, including the authentication of customers prior to disclosing CPNI
based on customer-initiated contacts. The Companies are committed to notify the FCC of any novel
or new methods of pretexting they discover and of any actions they take against pretexters and data
brokers.

Training and discipline

- The Companies trains their supervisory and non-supervisory personnel in an effort to ensure that their employees, in accordance with FCC regulations: (a) understand what CPNI is, (b) join in and carry-out the Companies' obligations to protect CPNI, (c) understand when they are and when they are not authorized to use or disclose CPNI, (d) obtain customers' informed consent as required with respect to its use for marketing purposes, and (e) keep records regarding receipt of such consent, customer complaints regarding CPNI and the use of CPNI for marketing campaigns.
- The Companies' employees are required to review the Companies' CPNI practices and procedures
 outlined in the Code of Conduct and to acknowledge their comprehension thereof.
- The Companies have an express disciplinary process in place for violation of the Companies' CPNI practices and procedures. The careless or intentional failure to comply with these practices and procedures may result in disciplinary action, up to and including discharge.

The Companies' use of CPNI

- The Companies may use CPNI for the following purposes:
 - To initiate, render, maintain, repair, bill and collect for services:
 - To protect their property rights, or to protect their subscribers or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
 - > To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent.
 - To market additional services to customers that are within the same categories of service to which the customer already subscribes:
 - > To market services formerly known as adjunct-to-basic services; and
 - To market additional services to customers with the receipt of informed consent via the use of optim or out-out, as applicable.
- The Companies do not disclose or permit access to CPNI to track customers that call competing service providers.

The Companies disclose and permit access to CPNI where required by law (e.g., under a lawfully issued subpoena).

Customer approval and informed consent

• The Companies do not use CPNI for marketing purposes. The Companies also do not share, sell, lease, or otherwise provide CPNI to any of their affiliates, suppliers, vendors, or any third parties for any type of service marketing purposes. If the Companies change this policy, they will implement a system to obtain approval and informed consent from its customers prior to the use of CPNI for marketing purposes. This system also will allow for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI. Records of approvals will be maintained for at least one year.

One time use

After authentication, the Companies may use oral notice to obtain limited, one-time approval for use of CPNI for the duration of a call. The contents of such notice will comport with FCC rule 64.2008(f).

Additional safeguards

- The Companies require supervisory approval for all marketing campaigns and maintain for at least
 one year records of such marketing campaigns, including a description of each campaign, the
 products offered as part of the campaign, and details of what information is used in connection with
 the campaign.
- The Companies designate one or more officers, as an agent or agents of the companies, to sign and file a CPNI compliance certificate on an annual basis. The certificate conforms to the requirements set forth in FCC rule 64.2009(e).
- For customer-initiated telephone inquiries regarding or requiring access to CPNI, the Companies authenticate the customer (or its authorized representative), through a dedicated account representative and a contract that specifically addresses the Companies' protection of CPNI. In the event a customer does not have a dedicated account representative, the Companies will authenticate the customer without prompting through the use of readily available biographical or account information, such as through the use of a pre-established password. If the customer cannot provide sufficient authentication, then the Companies only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record.
- The Companies do not permit online customer access to CPNI, nor do they have retail locations where customers may request access to CPNI.
- The Companies notify customers immediately of any account changes, including address of record.
 authentication, and password related changes.
- In the event of a breach of CPNI, the Companies will notify law enforcement as soon as practicable and no later than seven (7) business days from discovering the breach. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs the Companies to delay notification, or the Companies and the investigatory party agree to an earlier notification. The

Companies will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved, along with notifications sent to law enforcement and affected customers.